DIGI AMERICAS ALLIANCE MEMBERS

MINISTERIO TIC INAUGURÓ EL CENTRO DE OPERACIONES DE SEGURIDAD NACIONAL DE COLOMBIA (SOC) PARA BLINDAR LA CIBERSEGURIDAD DE LAS ENTIDADES DEL PAÍS

MinTIC - Pensando en prevenir, gestionar y responder rápidamente a los incidentes de ciberseguridad y amenazas emergentes, afianzar el conocimiento sobre la materia y fomentar una cultura de protección en el entorno digital, el ministro TIC, Mauricio Lizcano, inauguró el Centro de Operaciones de Seguridad Nacional (SOC). Esta iniciativa, liderada por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) del Ministerio TIC y apoyado por entidades clave del ecosistema digital del país, es un pilar clave de la estrategia nacional de ciberseguridad.

POLÍCIA FEDERAL DEFLAGRA OPERAÇÃO CONTRA QUADRILHA ESPECIALIZADA EM FRAUDES NA CAIXA - BRASIL

SBT News - A Polícia Federal (PF) deflagrou nesta quarta-feira (22) a operação Chaes, com objetivo de desarticular um grupo criminoso especializado em fraudes financeiras. O esquema afetava principalmente clientes da Caixa Econômica Federal, mas outras instituições bancárias também foram alvo da quadrilha. A investigação, que contou com o apoio da Coordenação de Repressão a Crimes de Alta Tecnologia (CCAT), revelou que o grupo usava um malware sofisticado chamado Chaes.

¿QUÉ TRAE 5G PARA LA CIBERSEGURIDAD? CLAVES PARA ENTENDER LOS RETOS Y OPORTUNIDADES - COSTA RICA

La Republica - La llegada del 5G representa un cambio de paradigma en la conectividad digital, ofreciendo mayor velocidad, menor latencia y una capacidad sin precedentes para conectar dispositivos, sin embargo, este avance tecnológico también trae consigo importantes desafíos en materia de ciberseguridad, de acuerdo con la Embajada China en Costa Rica.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 23, 2025

PN AVANZA EN EL DISEÑO ORGANIZACIONAL DE LA DIRECCIÓN DE ÁREA DE CIBERSEGURIDAD - REPÚBLICA DOMINICANA

CDN - La Policía Nacional (PN) realizó la tercera reunión de coordinación para la creación de la Dirección de Área de Ciberseguridad, en un encuentro efectuado en el Salón de Pensamiento Estratégico de la Dirección Central de Planificación y Desarrollo (Diplan). El encuentro tuvo como objetivo principal afinar los detalles estratégicos y organizacionales de esta nueva dependencia, diseñada para proteger los equipos, sistemas, datos y redes de la institución.

EEUU SANCIONÓ A FIRMA CHINA QUE APOYÓ CIBERESPIONAJE EN PARAGUAY

UltimaHora - Un grupo de ciberespionaje basado en la República Popular de China, identificado como Flax Typhoon, se infiltró en los sistemas del Gobierno paraguayo hace poco más de un mes. La Oficina de Control de Activos Extranjeros (OFAC, por sus siglas en inglés) del Departamento de Tesoro actualizó su lista negra de personas, entidades y embarcaciones que el Gobierno de los Estados Unidos considera que amenazan la seguridad nacional o la política exterior del país.

MÉXICO DEBE TRABAJAR MÁS EN TEMAS DE CIBERSEGURIDAD E INTELIGENCIA ARTIFICIAL PARA DETENER LA VIOLENCIA

Metropoli - México tiene que enviar buenas señales al exterior, que está trabajando en el combate al fentanilo, corrupción, impunidad, debido a que México permanece en una grave crisis de violencia del crimen organizado, principalmente en lo que se refiere a la violencia delictiva de alto impacto y la asociada a las disputas criminales por el control territorial. En una conferencia de prensa, expertos en seguridad realizaron un análisis de Seguridad 2025, un análisis Multidisciplinario, donde alertaron que México debe trabajar en temas de ciberseguridad, le urge apoyo en materia de seguridad, “porque no ha sido capaz de resolver su problema de violencia”.

ALCALDÍA DE PACHUCA REFUERZA CIBERSEGURIDAD TRAS INTENTO DE HACKEO - MEXICO

am - Luego de un presunto intento de hackeo a los sistemas del ayuntamiento de Pachuca, autoridades municipales emitieron un comunicado para informar las medidas que aplicarán a fin de evitar riesgos. El documento indica que habrá protección inmediata, pues desde la detección del incidente se activaron protocolos avanzados de ciberseguridad dirigidos por especialistas de la Dirección de Informática, lo que ha permitido proteger los sistemas y reducir riesgos.

TENDENCIAS DE CIBERSEGURIDAD E INTELIGENCIA ARTIFICIAL PARA 2025

Merca2.0 - El avance de la inteligencia artificial (IA) y las amenazas cibernéticas ha llevado a las empresas a un punto de inflexión en el que deben adoptar estrategias innovadoras para mantenerse protegidas...Identificado siete predicciones clave que marcarán el futuro de la ciberseguridad en 2025, destacando la convergencia de la IA y las plataformas unificadas como motores de cambio.

REALIDAD E IDENTIDAD FALSIFICADAS: NUEVO RETO DE CIBERSEGURIDAD

Debate - Los especialistas en ciberseguridad pronostican que en 2025 se producirá un salto importante en el uso de inteligencia artificial y ‘deepfakes’ (videos falsificados extremadamente realistas), el robo de datos experimentará un salto significativo evolucionando hacia el robo de identidad masivo, y surgirán estafas sofisticadas y nuevas tácticas de fraude financiero.

COORDINACIÓN Y GOBERNANZA EN CIBERSEGURIDAD: NUEVO MARCO NORMATIVO Y OPERATIVO - UE

CincoDias - Las normativas NIS-2 y DORA refuerzan la obligación de supervisar proveedores críticos, unificando la responsabilidad de estas entidades con la gestión integral de su ecosistema digital. Año nuevo, nuevos retos y con nueva normativa: NIS-2 y DORA. Vienen cambios, y con ello, dudas. Toca generar certidumbre. Toca generar crecimiento. Abordemos ideas-fuerza, tanto legales como operativas, que potenciarán la eficacia en la gestión corporativa.

CYBERSECURITY IN TRANSITION: BIDEN ADMINISTRATION WARNINGS AND WHAT’S NEXT FOR THE U.S.

Govtech - From a new White House executive order on cyber to a blog from the outgoing CISA director to more scary details on the Treasury hack, the outgoing administration has strong words on cyber threats. As President Joe Biden and his team of appointed senior executives across the federal government packed their bags and prepared to vacate offices inside the D.C. Beltway, one of their strongest messages proclaimed in their final days was this: "Pay attention on all things cybersecurity." President-elect Donald J. Trump takes the oath of office (for the second time) at noon EST on Monday, Jan. 20, 2025. Meanwhile, the Biden administration sent a string of last-minute directives and warnings regarding cybersecurity over this past week.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 23, 2025

TRUMP REVOKES BIDEN EXECUTIVE ORDER ON ADDRESSING AI RISKS - US

Reuters - U.S. President Donald Trump on Monday revoked a 2023 executive order signed by Joe Biden that sought to reduce the risks that artificial intelligence poses to consumers, workers and national security.
Biden's order required developers of AI systems that pose risks to U.S. national security, the economy, public health or safety to share the results of safety tests with the U.S. government, in line with the Defense Production Act, before they were released to the public.

COMMONWEALTH FELLOWS DEVELOP ROADMAP TO COMBAT CYBERCRIME IN CARIBBEAN

The Commonwealth - Commonwealth Caribbean cyber fellows have developed a roadmap this week, designed to boost around-the-clock cooperation to combat online crimes and make the internet safer for citizens.
The roadmap was the result of two days of discussions among 15 fellows, including officials from The Bahamas, Barbados, Grenada, Guyana, Jamaica, Trinidad and Tobago, the CARICOM Implementation Agency for Crime and Security, and the Regional Security System. The roadmap lays out a framework for greater regional cooperation to prevent and combat cyber threats, including fraud, ransomware, and hacking.

"ARTIFICAL INTELLIGENCE AND CYBERSECURITY: BALANCING RISKS AND REWARDS" WHITE PAPER

WEF - Cyber risks related to AI adoption have to be considered by business leaders and senior risk owners alike. This report is part of a series exploring the transformative role of artificial intelligence (AI) across industrial ecosystems, along with cross-industry, industry-specific and regional perspectives. It is specifically focused on how organizations can reap the benefits of AI adoption while mitigating the associated cybersecurity risks. The business benefits of adopting AI can be considerable, but the cyber risks of embedding these technologies into an organization are not always considered from the outset. By adopting AI, businesses may find themselves vulnerable to new threats that they do not yet know how to defend themselves against.

RESTORING TRUST ONLINE: WHAT CAN WE LEARN FROM CYBERSECURITY'S ZERO TRUST MODELS?

WEF - In recent years, cybersecurity engineers have been shifting into a new security model called "zero trust": the idea that trust should not be automatically granted to any user or device by default. This stance has not yet been adopted by digital societies. Online users often bypass the information verification step, as evident from the global rise of false and misleading information. By adopting principles from zero trust models, online users could use the power of emerging AI technology, together with human moderation, and blockchain technology to become better at verifying information.